REMARKS

In the current and final Office Action, claims 1-47 were examined.

Claims 1-47 were rejected.

Specifically:

Claims 1-2, 4-11, 13-28, 30-31, 33-35, and 37-42 were "rejected under 35 U.S.C. 102(e) as being anticipated by Downs et al (US 6,574,609)."

Claims 3, 12, 29, 32, 36, and 43-47 were "rejected under 35 U.S.C. 103(a) as being unpatentable over Downs et al. (US 6,574,609) as applied to claims 1-2, 4-11, 13-28, 30-31, 33-35, and 37-42 above, and further in view of Yoshida et al. (US 6,674,874).

I. It is respectfully submitted that no art of record (including Downs et al. and/or Yoshida et al.), either alone or in any combination, anticipates or renders obvious claims 1-43.

A. For example, (i) the secure container (SC) of Downs et al. includes usage conditions, and (ii) the license and/or certificate of Downs et al. does not include usage conditions.

1. Downs et al. reads at column 15, lines 21-24, in pertinent part:

> "And Usage Conditions 206 for content licensing management as described below. *The SC(s) 200 comprises Usage Conditions 206...*"
>
> (emphasis added)

2. Downs et al. reads at column 11, line 64 to column 12, line 9, in pertinent part:

> "The End-User Device(s) 109 manages the download and storage ofthe SCs containing the Digital Content; requests and manages receipt of the encrypted Digital Content keys from the Clearinghouse(s) 105; processes the watermark(s) every time the Digital Content is copied or played; manages the number of copies made (or deletion of the copy) in accordance with the Digital Content's Usage Conditions; and performs the copy to an external media or portable consumer device if permitted. The portable consumer device can perform a subset of the End-User Player Application 195 functions *in order to process the content's Usage Conditions embedded in the watermark.*"
>
> (emphasis added)

3. Downs et al. reads at column 14, lines 41-49, in pertinent part:

> "A digital certificate is used to authenticate or verify the identity of a person or entity that has sent a digitally signed message. A certificate is a digital document issued by a certification authority that binds a public key to a person or entity. The certificate includes the public key, the name of the person or entity, an expiration date, the namne of the certification authority, and other information. The certificate also contains the digital signature of the certification authority."

4. Downs et al. reads at column 28, line 63 to column 29, line 12, in pertinent part:

> "Clearinghouse(s) Certificate(s)--A certificate from a certification authority or from the Clearinghouse(s) 105 that contains the signed Public Key 621 of the Clearinghouse(s) 105. There may be more than one certificate, in which case a hierarchical level structure is used with the highest level certificate containing the public key to open the next lowest level certificate is reached which contains the Public Key 621 of the Clearinghouse(s) 105.
>
> Certificate(s)--A certificate from a certification authority or from the Clearinghouse(s) 105 that contains the signed Public Key 621 of the entity that created the SC(s). There may be more than one certificate, in which case a hierarchical level structure is used with the highest level certificate containing the public key to open the next level certificate, and so on, until the lowest level certificate is reached which contains the public key of the SC(s) creator."

5. Downs et al. reads at column 11, lines 18-24, in pertinent part:

> "Once these verifications are satisfied, the Clearinghouse(s) 105 sends the decryption key for the Content 113 to the requesting End-User(s)

packed in a License SC. The key is encrypted in a manner so that only the authorized user can retrieve it. If the End-User's request is not verifiable, complete, or authorized, the Clearinghouse(s) 105 repudiates the request for the decryption key."

6. Downs et al. reads at column 28, lines 14-16, in pertinent part:

"Usage Conditions--A part that contains information that describes usage options, rules, and restrictions to be imposed on an End-User(s) for use of the Content 113."

7. Downs et al. reads at column 9, lines 51-62, in pertinent part:

"A Metadata Assimilation and Entry Tool 161 is used to extract metadata from the Content Provider(s)' Database 160 (for a music example the Content 113 information such as CD title, artist name, song title, CD artwork, and more) and to package it for electronic distribution. *The Metadata Assimilation and Entry Tool 161 is also used to enter the Usage Conditions for the Content 113.* The data in Usage Conditions can include copy restriction rules, the wholesale price, and any business rules deemed necessary. A Watermarking Tool is used to hide data in the Content 113 that identifies the content owner, the processing date, and other relevant data."

(emphasis added)

8. Downs et al. reads at column 8, lines 13-29, in pertinent part:

"Digital watermarking also provides the means to identify the origin of authorized or unauthorized copies of Content. An initial watermark in the Content is embedded by the content proprietor to identify

the content proprietor, specify copyright information, define geographic distribution areas, and add other pertinent information. A second watermark is embedded in the Content at the End-User Device(s) to identify the content purchaser (or licensee) and End-User Device(s), specify the purchase or license conditions and date, and add any other pertinent information.

Since watermarks become an integral part of the Content, they are carried in the copies independent of whether the copies were authorized or not. *Thus the Digital Content always contains information regarding its source and its permitted use regardless of where the content resides or where it comes from.* This information may be used to combat illegal use of the Content."

(emphasis added)

B. Thus, no art of record, either alone or in any combination, anticipates or renders obvious at least the following elements in conjunction with the other elements of their respective claims:

Claim 1: **an authentication module configured to access a certificate, which indicates permissible uses of the digital content file, associated with and separate from the digital content file . . . .**

Claim 11: **associating the digital content file with a certificate that contains copyright information including at least one indication regarding a permissible use of the digital content file and is not a part of the digital content file.**

Claim 17: **configuring the certificate file with permissible use information about the digital content file so that when the digital content file is processed, the digital content file is**

processed in accordance with the permissible use information contained in the certificate file.

Claim 25: **if the watermark signal is detected, attempting to locate a certificate associated with the digital content file, the certificate including copyright information having at least one indication regarding a permissible use of the digital content file.**

Claim 30: **the certificate containing copyright information including at least one indication regarding a permissible use of the digital content file.**

Claim 35: **if the watermark is detected, attempting to locate a certificate that is associated with the digital content file, the certificate containing instructions regarding the digital content file . . . wherein the watermark only indicates the existence of the certificate.**

Claim 43: **wherein the 1-bit watermark indicates the presence of a certificate associated with the digital content, the certificate containing copyright information including at least one indication regarding a permissible use of the digital content and being stored apart from the digital content.**

Reasons for the allowability of independent claims 1, 11, 17, 25, 30, 35, and 43 have been provided above. Claims 2-10, 12-16, 18-24, 26-29, 31-34, 36-42, and 44-47 depend from these independent claims 1, 11, 17, 25, 30, 35, and 43, respectively. Although each also includes additional element(s) militating toward allowability, it is respectfully submitted that these dependent claims are allowable at least for the reasons given above in connection with their respective independent claims.

CONCLUSION

It is respectfully submitted that all of the pending claims 1-43 are allowable, and prompt action to that end is hereby requested.

Respectfully Submitted,

Date: 02/14/2005 By: Keith W. Saunders

Keith W. Saunders
Reg. No. 41,462
(509) 324-9256 x238